# TP2
# Attaque Man in the Middle

## 1 Objectif

Découvrir les attaques de type Man in the Middle

## 2 L'outil

### 2.1 Ettercap

**Ettercap** est un logiciel libre d'analyse du réseau informatique. Il est capable d'intercepter le trafic sur un segment réseau, de capturer les mots de passe, et de réaliser des attaques dites de l'homme du milieu (Man In The Middle) contre un certain nombre de protocoles de communication usuels tels que HTTP, FTP et certains protocoles chiffrés[1].

## 3 Plateforme du TP

Pour la réalisation de ce tp, on va adopter la plateforme illustrée au schéma suivant:

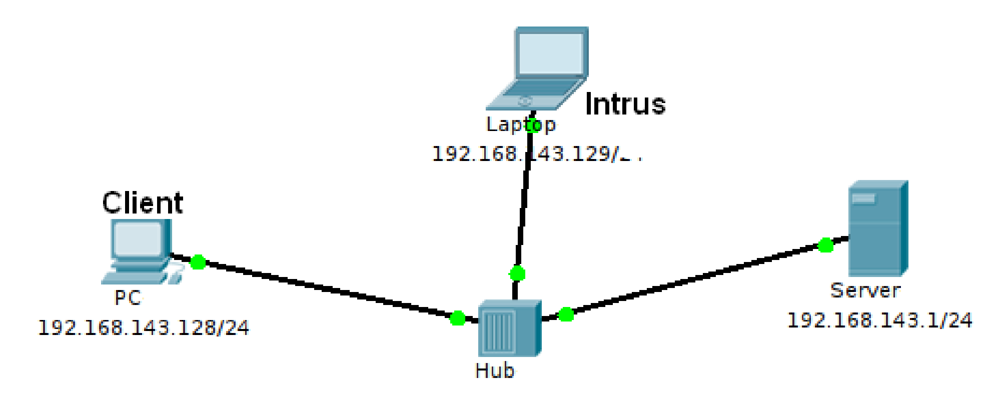



Figure 1: Réseau LAN

## 4 Usurpation ARP

Découvrez le réseau et choisissez deux machines à usurper

Notez leurs adresses mac

Vérifiez le cache arp de chaque machine: *arp* (-a pour les machines windows)

Lancez l'outil: *ettercap -G*

Sélectionnez le mode de "reniflement": Sniff → Unified sniffing

Choisissez l'interface de votre convenance

Découvrez les machines actives de votre LAN: Hosts → Scan for hosts

Affichez la liste des machines actives: Hosts → Hosts list

Sélectionnez les machines à usurper

[1] Wikipédia

Vérifiez les cibles: Targets → Current targets

Démarrez l'usurpation ARP: MITM → Arp poisoning

Démarrez le sniffing: Start → Start sniffing

# 5 Usurpation DNS

**Préparation de l'attaque**

Toujours avec la même plateforme

On commence par une usurpation ARP (on se met entre la machine de la victime et la passerelle vers internet)

La première chose à faire est d'éditer le fichier */usr/share/ettercap/etter.dns*

Ajoutez ces lignes

> *.google.co.in A 192.168.1.12
>
> *.google.com A 192.168.1.12
>
> google.com A 192.168.1.12
>
> www.google.com PTR 192.168.1.12
>
> www.google.co.in PTR 192.168.1.12

Cela signifie que lorsque vous essayerai d'ouvrir *google.com* vous allez vous adresser à la machine 192.168.1.12

**Démarrage de l'attaque**

Explorez les plugins: Plugins → Manage the plugins

Vérifiez les caches des machines usurpées